1449 nor has a copy of Shear been provided to Applicant.

A. The Present Invention

The present invention discloses an extended X.509 certificate capable of supporting more than one cryptographic algorithm. The certificate comprises a signature algorithm and a signature for all authenticated attributes using a first cryptographic algorithm, and alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

B. Differences Between the Present Claims and the Cited Art

The Office Action identifies a passage from Shambroom as disclosing "a certificate that supports one or more cryptographic algorithms" and that "the certificate can resemble an X.509 certificate," citing Column 10, lines 32-35

More specifically, Shambroom states that "web server 720 responds with a certificate to web browser 620. This certificate contains the network server's public key and a list of one or more cryptographic algorithms that the network server supports..." (Column 10, lines 30-34).

The key here is that the Shambroom certificate contains a **list** of one or more cryptographic algorithms that the **network server** supports. The Shambroom certificate does not actually use or employ multiple cryptographic algorithms to protect the data therein. The Shambroom data appears to be the list of algorithms. The certificate in Claim 1 does **not** contain a list of cryptographic algorithms that a network server supports. The claimed certificate utilizes and uses more than one cryptographic algorithm itself to protect the data it includes.

Further, the network server's public key appears to be used by the web browser to log

onto or communicate with the web server 720, which is part of the network server 700, and not to protect the data in the certificate. In other words, the Shambroom certificate is used to transfer data, including the list of cryptographic algorithms that the network server supports and the public key for the network server, to the web browser. No such scheme is contemplated by the present invention.

The Office Action goes on to state that the "list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm." This statement is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

Claim 1 recites that the X.509 certificate comprises "a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;" as well as "an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and an alternative signature extension for containing a signature for the alternative cryptographic algorithm." This is not the same thing as a list of cryptographic algorithms that a network server supports as per Shambroom, and such a list included in a certificate does not teach, suggest or disclose the subject matter of Claim 1. Shambroom does not teach that its certificate protects its data using more than one cryptographic algorithm. The Shambroom list appears to be data included in the certificate, not multiple cryptographic algorithms employed by the certificate to protect its data, as per Claim 1.

Schneier appears to describe a standard X.509 certificate which employs a single cryptographic algorithm. Applicant notes that portions of pages 480, 481, 574 and 575 of Schneier were not legible in the photocopies provided with the Office Action.

Including a list of cryptographic algorithms as data in a certificate does not teach, suggest or disclose using multiple algorithms to protect the data in the certificate. There is no reason to combine Shambroom's list of cryptographic algorithms contained in a certificate (which indicate which algorithms a server supports) with the standard X.509 certificate, such as that of Schneier, which actually uses a single algorithm to protect data contained therein.

The current Office Action introduces the Shear reference in rejecting Claim 1. Shear is directed to security for load modules. In the Abstract, Shear states that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise."

However, Shear does not suggest, teach or disclose creating extensions to a certificate. The Office Action argues that it would be obvious to put multiple signatures formed with different algorithms into Shambroom's certificate based on the teachings of Shear.

Applicant has never argued that the present invention claims the concept of using more than one algorithm for the purpose of security. Rather, Applicant has figured out how to make such a multiple algorithm system work with respect to certificates. This involves the use of extensions. And none of the references teaches this or mentions the use of extensions in such a manner. None of Shambroom, Shear and Schneier discusses the use of extensions to enable the certificate to support an alternative cryptographic algorithm, as per the second and third elements of Claim 1.

Accordingly, Applicant submits that Claim 1 patentably distinguishes over the combination of Shambroom, Shear and Schneier. Accordingly, dependent Claim 2 and 3 should also distinguish over the cited art.

C Improper Combination of References

Additionally, the Examiner has failed to provide a convincing line of reasoning for combining the teachings and structure of Shambroom with the teachings and structure of Schneier and the teachings and structure of Shear so as to arrive at the present claimed invention. Under 35 U.S.C. Section 103, when the Examiner has relied on the teachings of several references, the test is whether or not the references viewed individually and collectively would have suggested the claimed invention to the person possessing ordinary skill in the art. See In re Kaslow, 707 F.2d 1366, 217 USPQ 1989 (Fed. Cir. 1983). It is to be noted, however, that citing references which merely indicate that isolated elements and/or features recited in the claims are known is not a sufficient basis for concluding that a combination of claimed elements would have been obvious. That is to say, there should be something in the prior art or a convincing line of reasoning suggesting the desirability of combining the references in such a manner as to arrive at the claimed invention. See In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986).

Applicants submit that there is no teaching in the reference or a convincing line of reasoning provided by the Examiner to combine the teachings of Shambroom, Shear and Schneier so as to arrive at the present claimed invention. Shambroom discloses a certificate that contains a **list** of one or more cryptographic algorithms that a **network server** support. Schneier describes a standard X.509 certificate which employs a single cryptographic algorithm. Shear is directed to security for load modules which uses several dissimilar digital signature algorithms. No reason is provided for combining a certificate which carries a list of algorithms (Shambroom) with a standard X.509 certificate (Schneier) with the concept that multiple dissimilar digital signature algorithms may be used for security for load modules. How and why anyone would combine these references so as to arrive at the present claimed invention is entirely unclear. Certainly, nothing is provided in the references that would suggest combining these references. No appropriate line of reasoning is provided for combining these references. Accordingly, Applicant submits that the combination of references is inappropriate and improper and respectfully submit that this is a further reason to overturn the rejection that stands alone from the reasons discussed above relative to the content of the references.

II. Traversal of the Rejection under 35 U.S.C. Section 101

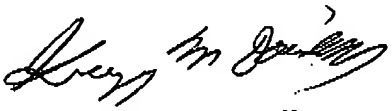
Claims 1 - 3 were newly rejected under 35 U.S.C. Section 101 for being directed to non-statutory subject matter. The rejection states that the claims claim data.

Applicant submits that the claims are statutory. The claims recite a functional structure for data. The claims do not recite sales data or a list of addresses. For example, in the Shear patent cited by the Examiner, Claims 14 and 34 recite a security structure.

III Summary

Applicant has presented technical explanations and arguments fully supporting his position that the pending claims contain subject matter which is not taught, suggested or disclosed by Shambroom, Schneier, Shear or any combination thereof. Accordingly, Applicant submits that the present Application is in a condition for Allowance. Reconsideration of the claims and a Notice of Allowance are earnestly solicited.

Respectfully submitted,



Gregory M. Doudnikoff
Attorney for Applicant
Reg. No. 32,847

Docket No: RSW9-98-0095
PHONE: 919-254-1288
FAX: 919-254-4330